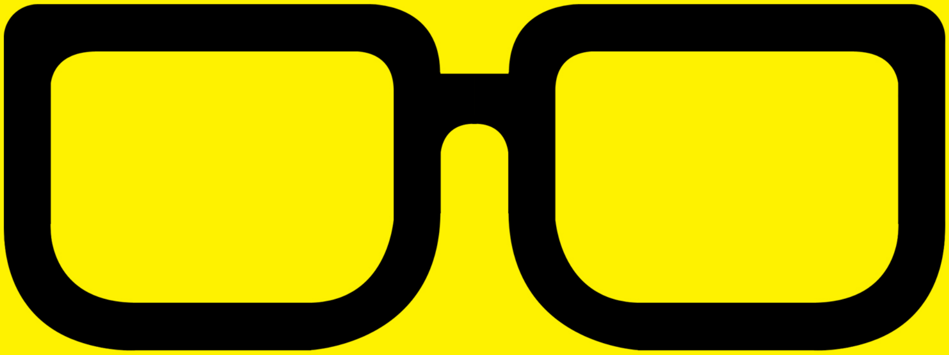
SPONSORED BY

helpsystems

GEEK GUIDE



Childhood's End: Attackers Increasingly Take Aim at Linux Systems

LINUX™ JOURNAL

Table of Contents

JOHN S. TONELLO is the Director of IT and Communications Manager for NYSERNet, New York's regional optical networking company, serving the state's colleges, universities and research centers. He's been a Linux user and enthusiast since building his first Slackware system from diskette more than 20 years ago. You can follow him @johntonello.

GEEK GUIDES:
Mission-critical information for the most technical people on the planet.

Copyright Statement

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of *Linux Journal* or its Web site sponsors. In no event shall *Linux Journal* or its sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

About the Sponsor

HelpSystems

HelpSystems makes IT lives easier by meeting critical needs like IT and business process automation, and system security. Stand Guard Anti-Virus is a malware protection solution that runs natively on Linux, avoiding the scan failures and security issues often caused by software designed for Windows. To further reduce system vulnerabilities, Policy Minder is a security monitoring solution that makes it easy to maintain security policies that follow the rule of least privilege.

For more information on Stand Guard Anti-Virus, see https://www.helpsystems.com/products/virus-protection-software-linux-aix-and-ibm-i.

For Policy Minder, visit https://www.helpsystems.com/products/security-policy-management-software-ibm-i-unix-linux-and-aix.

Childhood's End: Attackers Increasingly Take Aim at Linux Systems

JOHN S. TONELLO

Like the wide-eyed humans who mistakenly trust their benevolent alien overlords in Arthur C. Clarke's science-fiction classic, Linux users the world over are beginning to awaken to the reality that their malware-free utopian childhood is rapidly coming to an end.

A startling increase in malware, ransomware and malicious code targeting Linux systems of all shapes and sizes since 2015 means the days of believing it's "just a Windows thing" are over. One study found that

Linux malware now accounts for more than 35% of all malware, and anyone not taking Linux security threats seriously can face real—and expensive—problems.

Korean web-hosting service provider Nayana found that out when it was attacked by Erebus, ransomware named for the Greek goddess of darkness. Nayana reportedly agreed to pay more than $1 million to regain access to maliciously encrypted data on 153 of its Linux servers hosting more than 3,400 customer websites.

Another bit of malware called Mirai turned thousands of vulnerable Linux-based routers, IP cameras and other IoT devices into a botnet that targeted Dyn and others with a massive DDoS attack.

In these cases and many others, Linux systems were the primary targets. Leading antivirus software makers report attacks on Linux systems have tripled in the last three years, with attackers of all skill levels seeing opportunities to exploit Linux directly—no longer content with targeting only Windows hosts.

The Conventional Wisdom

Linux users always have boasted of the "what, me worry?" advantage of how the OS is built. They tend to argue that they have three big advantages over Windows:

- The open-source OS they know and love is fundamentally more secure.
- Vast seas of Windows desktops draw attackers' more serious attention.

Although largely true, this level of confidence requires the Linux systems in question to be up to date and well patched, and managed by disciplined admins who limit privileged access.

- The Open Source community is essentially a big brain that's quick to solve problems.

These folks also tend to argue that careless desktop users introduce most malware threats by clicking on email links and attachments that they shouldn't.

Although there's truth in all these points, the reality is far more complicated. When it comes to security—on any platform—there are no absolutes.

Take the Linux filesystem. Linux users old and new always have been told Linux is far more secure and far less vulnerable than Windows systems, because the filesystem permissions at the heart of Linux reduce—and often eliminate—most risks. Attackers, they argue, simply can't get past this fundamental aspect of Linux boxes.

Although largely true, this level of confidence requires the Linux systems in question to be up to date and well patched, and managed by disciplined admins who limit privileged access. In the 2017 attack, Erebus infected Nayana Linux hosts running the 2.6.24.2 kernel, Apache 1.3.36 and PHP 5.1.4. These kernel, web server and scripting language versions are more than eight years old and littered with exploitable vulnerabilities.

A Worthy Target in Its Own Right

Conventional wisdom has always presumed the attack surface for Windows is far greater, both in scale and opportunity, than Linux. One of the "victories" of owning the desktop has made Microsoft OSes the overwhelming target for viruses. The number of Windows-based PCs, many argue, gives attackers orders of magnitude more machines to enlist and compromise. Coupled with most end-users' malware apathy, this adds up to millions of computers ripe for the picking.

On the surface, they're right. The WannaCry malware targeted WinXP systems in more than 100 countries and successfully compromised at least 75,000 computers. That seems like a big number until you compare it with the estimated 500,000 Linux-based IoT devices infected by Mirai a year earlier.

As these attacks make clear, Linux is offering attackers new opportunities that conflict with the conventional wisdom that the vast majority of malware enters networks and systems when email users click on links or download things they shouldn't. SambaCry, a code-execution vulnerability found in all versions of Samba since 3.5.0, allows a remote user to execute code on a CIFS host. That means an attacker could use the popular file- and printer-sharing tool to target innumerable host servers. Left unpatched, the vulnerability could enable ransomware-style encryption or other malicious code on a wide variety of Linux machines, particularly Linux-based NAS devices that may be running custom branches that are harder to patch.

Making matters worse, new tools and something dastardly called Malware as a Service mean that even amateur attackers can bang away at Linux systems the world over and find their way to making your life hell.

These so-called MaaS sites created by black-hat attackers allow amateurs to buy sophisticated malware tools that give them powers beyond their own meager abilities. Many of these tools target dated, unpatched systems, which all but broadcast their vulnerabilities with basic port scans. Automated nmap scans reveal an awful lot. If you've never played with nmap, try this from any Linux shell:

```
# nmap -A -T4 yourwebsite.com
```

That simple command can show the remote system's OS, open ports, the version of the web server you're running (such as Apache, nginx or Varnish), the HTTP generator (such as Drupal or WordPress) and its version, when your SSL certs expire and more. Thanks to Malware as a Service, now amateurs have access to tools that turn simple utilities into hard-charging threats.

Facing the New Reality

In 2017, it's hard to find even the smallest IT shop without some sort of Linux. For many, Linux is at the core of their operations, providing everything from file shares to websites and databases to KVM hosts to network-attached storage devices. If you have assets in AWS, Google Compute Engine, Azure or other cloud vendor, chances are, Linux is fundamental to all you do there too. As a result, your Linux systems aren't an afterthought. They're an integral part of your environment.

With improved tools, Linux and Windows systems have grown to play well together, but the same seamless connections that make that seamlessness an admin's dream are now creating new worries.

That's because even the most well patched and well managed Linux systems can become malware carriers. That is, Samba-based CIFS file shares can pass along viruses without becoming infected themselves, spreading malware across your networked infrastructure.

Scanning these shares with Windows-based antivirus tools can ferret out some of the malware, but it can open other vulnerabilities. If a permanent Samba share mounted on a user's Windows 10 desktop is part of a nightly scan, you may be scanning unencrypted files across your network, exposing files to sniffing that can compromise secure files, passwords and sensitive data.

At the same time, "local" scans of remote systems often tempt—or require—you to grant a Windows PC greater permission than you would grant a typical Windows user. If that's the case, you could be adding risk. If you've centralized the file-share scans on, say, a Windows server instead of locally, a network or power outage could quietly halt the scans.

Fortunately, there are a number of alternatives to the sort of piecemeal approach many rely on to keep their Linux machines free of malware, including automation tools, native-OS antivirus software and updated awareness.

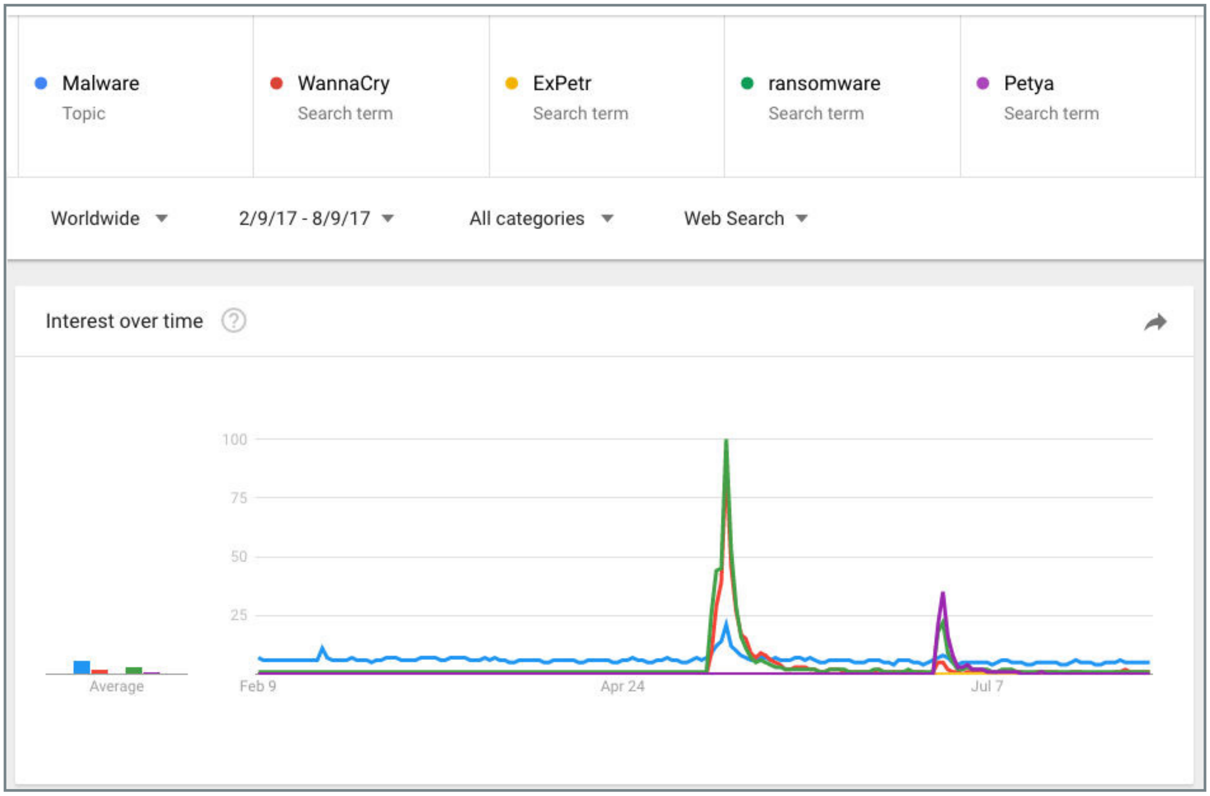
Arming Yourself with a Few Basic Countermeasures

By far, the greatest attack surfaces for would-be Linux attackers are unpatched kernels and packages. If you're not regularly running updates, applying timely patches and paying attention to security news, you're not trying hard enough. After all, you can automate updates—particularly security updates—pretty easily these days with native Linux tools or third-party apps like Ansible, Chef or Puppet. There's really no excuse for running a ten-year-old version of Apache or FTP or SSH server, and it's really asking for it.

Of course, your users continue to be a large source of risk, but it's not just end users who don't pay attention to malware risks. Admins can be just as guilty—particularly if they assume they have no risk in the first place.

A good example of this is clear if you take a look at Google trends in routine searches for "malware", "ransomware", "WannaCry", "ExPetr" and "Petya". Almost no one Googled malware terms until the WannaCry virus hit, but even then, interest peaked at 21 (out of 100). Ransomware searches went from a steady 0 or 1 to 100 on May 15, 2017, when WannaCry was in mid-stride, but the interest waned nearly as quickly as it appeared, returning to near 0 less than two weeks later.

Granted, Google searches alone can only hint at what people are thinking and worrying about, but you don't have



● Malware
Topic

● WannaCry
Search term

● ExPetr
Search term

● ransomware
Search term

● Petya
Search term

Worldwide ▾ 2/9/17 - 8/9/17 ▾ All categories ▾ Web Search ▾

FIGURE 1. **People just aren’t generally curious about daily malware risks, according to Google search activity. Searches peaked for “ransomware” and “WannaCry” when international media carried the story, but they quickly faded back to nil (source: https://trends.google.com/trends/explore?date=2017-02-09%20 2017-08-09&q=%2Fm%2F0582c,WannaCry,ExPetr,ransomware,Petya).**

to be a Big Data scientist to know that most people are content with what they already know—or think they know—about malware, its variants and its risks. If your users aren’t paying attention, surely you must be, particularly if you’re in a highly regulated industry, such as healthcare, finance or higher education where privacy is paramount.

If you're subject to the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA) or the Payment Card Industry Data Security Standard (PCI DSS), not adhering to security and data privacy standards can cost you three ways: in lost data, fines and credibility.

How Attacks Happen and How to Avoid Them

In case you missed it, hubris can be a Linux user's greatest downfall, but it's only one of the top security risks to keep in mind and mitigate.

Don't Presume Linux Is Not a Target and Do Nothing Surely, we've moved past this extreme level of complacency, but I'd be willing to bet there are many people who believe in the immutability of their Linux systems and do nothing. Think of Java and other cross-platform tools. They're designed to work on a variety of platforms unmodified. That means they can be executed on Linux systems and wreck havoc—even on well maintained ones. Don't presume Linux is more secure than Windows and, therefore, presume Linux is 100% secure. Again, OS bias (or just outdated knowledge) can blind admins to risks to their beloved Linux systems.

Recognize That Files on Any Platform Can Be Encrypted and Locked for Ransomware Malware today is not just for Windows any more. Files on any filesystem—Windows, Mac, Linux, IBM i and AIX included—are vulnerable. You don't have to look far for examples of comprised or maliciously encrypted files on all of those platforms. Linux never was fully immune and is less so today.

Unpatched Software, Including SSH and Common Services Like Apache and FTP, Create Vulnerabilities Regular updates and patching work to lower your risks dramatically. Still, many people don't do them, perhaps for fear of "breaking" apps that rely on older versions of, say, PHP. If you're not updating your systems for fear of breaking old custom apps, you need to do some soul-searching. Does the cost of redeveloping an app outweigh the security risk? Do the math and decide—soon.

Unpatched Services atop Other Services Are Entry Points for Malware, Regardless of OS Platform Content management systems like Drupal and WordPress have given end users powerful tools to manage websites and content, and new modules and plugins make them more useful each day. Unfortunately, many of those third-party tools have hooks right into your servers' most powerful permissions—including FTP write access—but aren't always well built. They provide entry points for attackers, so patching Apache, nginx or Varnish isn't enough. You need to stay on top of the services running on top of those services to make sure you're protected fully.

Linux Systems Can Be "Resistant Carriers" That Pass Viruses and Malware to Vulnerable Systems If you believe there are no native viruses lurking on your Linux machines, you're mistaken, and if you believe your Linux machines can't become a carrier for Windows malware, you're wrong too. You need native-OS virus tools (and signature files and heuristic detection) to look for and

Using a local, Linux-based scanning tool not only gives you better insight into UNIX-specific threats, but it eliminates the inherent risks of running scans across a network.

remediate both kinds of threats, particularly threats living in a Linux filesystem that PC-based scan engines can't uncover.

Remote, Non-Native Scans Can Leave Linux Filesystems Open and Vulnerable Linux Samba shares do a good job of helping you forget they're Linux. After all, they look like and behave like any other Windows share. But, remote Windows antivirus tools invite permission vulnerabilities, don't necessarily scan for Linux-native malware, may die with a network or power hiccup, and hammer your network if you're scanning large directories or big files.

Using a local, Linux-based scanning tool not only gives you better insight into UNIX-specific threats, but it eliminates the inherent risks of running scans across a network. If the remote scanning PC or your network fail, so does your scan. You can avoid those hassles and speed up scanning with native solutions that don't rely on network limitations. Perhaps most important, Linux-native tools are designed for Linux, and they use signature files and heuristic analysis designed to detect Linux-specific threats.

Unencrypted Remote Shares Can Leave Network Traffic Vulnerable If you're relying on Windows tools to scan the contents of Linux shares over a network, that traffic can be sniffed and exposed. You might say, "Who cares? Only my team has access and I trust them." Yes, but some of the biggest hacks ever perpetrated were done by disgruntled employees looking to do harm or other insiders looking to make a few bucks selling data. Don't get too paranoid, but always keep the rule of least-privilege in mind.

Don't Let the Scale of Your Operation Keep You from Monitoring Everything Virtualization and containerization have made it easy to spin up new hosts across your entire infrastructure, on-premises and off. This scale can be particularly difficult to manage and keep track of, especially if you haven't automated or otherwise standardized deployments and patching. If this sounds like you, it's seriously time to consider automation and a native-OS malware scanning tool that can scan all your Linux hosts systematically—wherever they live—and keep you in the know.

It takes only a single vulnerable container with a few exposed ports to offer attackers a way into your network. Manually checking logs on a dozen machines might work for now, but as the number of hosts grows, you can't rely on human analysis alone—unless, of course, you have an unlimited budget to hire new staff!

If you've brewed up a quiver full of scripts that automate basic tasks like setting initial firewall rules or system users, that's great—if you have only a few hosts. If you've grown beyond a handful of servers or appliances, consider tools like Ansible, Chef and Puppet to move your automation to the next level. If you could check for updates reliably or, say, look for old versions of Apache on all your systems all at once with a few simple lines of code, wouldn't you do so?

Open-source versions of these and other tools are readily available, can help you keep things current and give you a nice documented audit trail that can prove it.

Create Policies That Limit Remote Root and Power-User Access If you're deploying Linux Samba shares or other connections between systems, be sure to have well defined user and group policies that follow the least-privilege rule. That is, don't create vulnerabilities by taking shortcuts with who has access to what. You can save yourself a lot of heartache and pain by investing time up front to make sure you're not setting yourself up to attacks.

Also, if you're moving data in the clear—even just across your LAN—take steps to encrypt it. Establishing machine-level firewall rules and deploying certificates aren't hard to do, but they can really harden your systems and thwart attackers.

Continue to Educate Users and Admins Attacks and threats are frustrating to any systems administrator or IT practitioner because they take valuable time away from far more valuable work. It's tempting to blame end users and careless admins, but that's no solution. It's far better to develop a culture of vigilance that rewards users for recognizing threats rather than laughing them off as loons.

Conclusion

The reality today is that the great things about Linux that have made it a stalwart in machine rooms the world over are now the very things that make the OS a legitimate target for attackers. By accepting that reality and taking a few simple steps, you can lower your vulnerability and risk dramatically—and feel more confident too.■

Resources and Further Reading

4 Reasons You Need Native Virus Scanning: https://www.helpsystems.com/powertech/resources/articles/you-need-native-anti-virus

When Malware Attacks Your IBM i, AIX, and Linux Servers: https://www.helpsystems.com/resources/guides/when-malware-attacks-your-ibm-i-aix-and-linux-servers

Three Reasons Your Need an Updated Security Policy: https://www.helpsystems.com/resources/articles/three-reasons-you-need-updated-security-policy

Linux malware: Leak exposes CIA's OutlawCountry hacking toolkit: http://www.zdnet.com/article/linux-malware-leak-exposes-cias-outlawcountry-hacking-toolkit

Linux malware gaining favor among cybercriminals: https://www.scmagazine.com/linux-malware-gaining-favor-among-cybercriminals/article/671935

Over 104,000 Samba installations vulnerable to remote takeover attacks: https://www.bleepingcomputer.com/news/security/over-104-000-samba-installations-vulnerable-to-remote-takeover-attacks